AMENDMENT TO THE CLAIMS

1. (Original) A method for facilitating secure data communications using a secret key for encrypting data flowing between first and second entities over a communications link, the method comprising: determining that the communications link has been idle; determining that there is data to flow over the previously idle communications link; and responsive to determining that there is data to flow over the previously idle communications link, initiating generation of a new secret key, the new secret key for encrypting data sent between the first and the second entities over the communications link.

2 - 38. (Cancelled)

39 (Newly added) A method performed at a first entity for facilitating secure data communications by using a secret key for encrypting data flowing between said first and a second entity over a communications link, the method comprising the steps of:

determining that the communications link has been idle;

determining whether data is available for flow over the previously idle communications link; and

in response to a determination that data is available, initiating generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link.

40 (Newly added) The method of claim 39 wherein the step of determining that the communications link has been idle includes the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating generation of a new secret key is performed only if the communications link is found to have been idle for at least the predetermined period of time.

41 (Newly added) The method of either claim 39 or claim 40 including the additional steps of:

determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and

if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key.

42 (Newly added) The method of claim 40 including the additional steps of:

sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and

monitoring the communications link for receipt of an acknowledgement from the second entity.

43 (Newly added) The method of claim 42 including the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time.

44 (Newly added) An apparatus for facilitating secure data communications by using a secret key to encrypt data flowing over a communications link between the apparatus and a remote system, said apparatus comprising:

a data detector for determining whether the communications link has been idle and whether data is now available for flow to the remote system over the communications link;

key generation logic responsive to determinations that the communications link has been idle and there is data now available for flow to the remote system to initiate generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link.

45 (Newly added) The apparatus of claim 45 further including a timer for determining whether the communications link has been idle for at least a predetermined period of time and wherein said key generation logic initiates generation of the new secret key only if the timer indicates that the communications link has been idle for at least the predetermined period of time.

46 (Newly added) The apparatus of either claim 45 or claim 46 further including a byte measurer for determining whether the amount of data sent over the communications link has exceeded a predetermined amount threshold since the last generation of a secret key and wherein the key generation logic initiates generation of a new secret key if the determination is that the amount of data sent has exceeded the predetermined amount threshold.

47 (Newly added) The apparatus of claim 46 further including a heartbeat issuer for sending a heartbeat to the remote system if the data detector determines that the communications link has been idle but there is no data available for flow to the remote system over the communications link.

48 (Newly added) The apparatus of claim 47 further including a detector for monitoring the communications link for an acknowledgment of the heartbeat from the remote system.

49 (Newly added) The apparatus of claim 48 further including a connection terminator for terminating the communications link if the detector fails to detect an acknowledgment of the heartbeat from the remote system within the predetermined period of time.

50 (Newly added) A program product comprising a computer usable media embodying program instructions which, when executed in a computer, results in the computer facilitating secure data communications with a remote system by using a secret key for encrypting data flowing between the computer and the remote system over a communications link by:

determining that the communications link has been idle;

determining whether data is available for flow over the previously idle communications link; and

in response to a determination that data is available, initiating generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link.

51 (Newly added) The program product of claim 50 further including program instructions for determining whether the communications link has been idle for at least a predetermined period of time and for generating a new secret key only if the communications link is found to have been idle for at least the predetermined period of time.

52 (Newly added) The program product of either claim 50 or claim 51 including additional program instructions for:

determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and

initiating generation of a new secret key if the amount of data sent is determined to have exceeded the predetermined amount threshold.

53 (Newly added) The program product of claim 52 including additional program instructions for:

sending a heartbeat message to the remote system only if it is determined that the link has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and

monitoring the communications link for receipt of an acknowledgement from the remote system.

54 (Newly added) The program product of claim 53 including an additional program instruction for terminating the communications link with the remote system if no acknowledgement is received from the remote system within a predetermined period of time.

Respectfully submitted,

/Gerald R. Woods/
Gerald R. Woods
Reg. No. 24,144
(919) 543-7204

Customer Number 25259
IBM Corporation
T81/503
P.O. Box 12195
Research Triangle Park, NC 27709-2195